Extractivism at Your Fingertips

Chagnon, Christopher Wetherel

Routledge
2021-05-31

Chagnon , C W , Hagolani-Albov , S & Hokkanen , S M 2021 , Extractivism at Your Fingertips . in J Shapiro & J-A McNeish (eds) , Our Extractive Age : Expressions of Violence and Resistance . 1st edn , Routledge Studies of the Extractive Industries , Routledge , Abingdon , pp. 176-188 . https://doi.org/10.4324/9781003127611 , https://doi.org/10.4324/9781003127611

http://hdl.handle.net/10138/332807
https://doi.org/10.4324/9781003127611

9

EXTRACTIVISM AT YOUR FINGERTIPS

Christopher W. Chagnon, Sophia E. Hagolani-Albov, and Saana Hokkanen

Introduction

The twenty-first century has seen a meteoric rise in the use and availability of technology aimed at individuals, by which we mean technology that is developed and deployed to be used by individual consumers. This technology includes personal computers, smartphones, tablets, and other handheld digital devices. Veiled by entertainment, interpersonal communication, and quick or convenient access to products and knowledge, an underlying and ever-present agenda involves collecting data about the individual using the device. The consumer becomes both the resource for collecting data and the target of the potential uses and abuses of the data collected. In this chapter we explore the infiltration of extractivist logic into the relationship between those providing the digital infrastructure and consumers in the digital realm. Extractivist logics are inextricably bound up with capitalism and other configurations of modernity—and with extractivism comes violence.

There are distinct modes of violence that unfold throughout the digital realm that are directly related to violence perpetrated in natural resource extraction, for example effects of mining lithium for the batteries used in digital devices. By drawing extractivist logic into the digital realm, new forms of violence are unleashed, that are often insidiously indirect and even manifestly unrecognizable, but are no less damaging on the socio-spiritual and physical levels. There are many unknowns in regard to effects or even potential violence that could be perpetrated against individuals when their personal data is accumulated in mass and deployed against them or monetized (Segura and Waisbord, 2019).

In this chapter we contribute an analysis of an ever more complex web of extractivisms. Here different forms of digital and data extractivism are observed to intersect with natural resource and financial extractivisms in their underlying logic and processes. We highlight how this complex web needs to be analyzed in the

modern era, to uncover the linkages and extensions of extractivist violence. The extractivist logic continues to expand into arenas where the extent of the infiltration of extractivist modes of operation has only recently been recognized.

Expanding Extractivisms

Not all scholars and activists are in accord with the push to expand understandings of extractivism. For example, Gudynas (2018) maintains that expanding the concept of extractivism beyond the realm of natural resources—to finance, or additional forms of development—is detrimental to the analytical and descriptive power of the concept, and thus undermines the search for alternatives. However, from an historical-ontological perspective the concept of extractivism rests upon a universalizing "natural law" in which the exploitation of "nature" features as an ontological prerequisite to the forms that European modernity developed over the last 500 years (see Chapter 1). As Mezzadra and Neilson (2017) note, new forms of financial and digital processes facilitate the expansion of resource extraction in the global economic system. The digitization of finance and data render these sectors of the global economy dependent on one another in increasingly complex ways. Monetarily, the most significant extractions currently take place on the digital platforms of global financial speculation, largely run by algorithms, through a computerized system with vast violent consequences for the everyday lives and livelihoods of beings around the world. The links to this digital realm and the rise of non-productive capital as the key sectors of capitalist expansion since 1990 are often hard to discern (Dowbor, 2018). What matters here are the logics, mindsets, and ideologies that stem from extractivist ontological dispositions (see Chapter 1), rather than the particular resource or technology. Moore (2018) argues this in his critique of Eco-Marxist theories (e.g. Malm, 2016) that place the most emphasis on coal in the surge of industrial capitalism. Indeed, the existence and prominence of less directly visible or tangible extractivist thrusts behind all sorts of tangible and mindset transformations fit in neatly with Dunlap and Jakobsen's conceptualization of "total extractivism," which is "centered on the deployment of violent technologies aiming at integrating and reconfiguring the earth and absorbing its inhabitants, meanwhile normalizing its logics, apparatuses and subjectivities, as it violently colonizes and pacifies various natures" (2020, p. 6).

This expanded and deepened understanding of extractivism guides attention towards the centrality of extractivist practices and mentalities within the broader modern world-system, and even during prior millennia of empire and civilization-buildings. This conceptualization also uncovers the expansionary and totalizing nature of extractivist thrusts. A central aspect of this global extractivism emphasized by Dunlap and Jakobsen (2020) is the centrality of coercion and social pacification, which enables rolling out and continuation of extractivist practices and the resulting environmental degradation. Violence and militarization are identified as the main mechanisms of coercion and social pacification (Dunlap and Jakobsen, 2020). However, there are types of violence(s) that play out against the human psyche,

which are also central to the overarching violences associated with extractivism. In data extractivism, these assaults to the psyche occur through increased exposure to algorithms and programs designed to make users dependent and catch their attention repetitively in digital realms. This results in the parallel process of data extractivism via extraction of knowledge of personal and human tendencies of behavior, and other processes that could be likened to digital colonialism (Thatcher *et al.*, 2016).

As forms of social control, data extractivism and data violence are becoming ever more necessary for extractivism, as they are used to discipline, to convert the subjectivities of people, and to supersede alternative relations between people and their environments. In addition, pro-corporate digital campaigns and resistance campaigning are becoming ever more central in politics, including electoral politics and contentious politics around natural resources (Kröger, 2013; 2020). These sorts of "positive mechanisms" of control (following Foucault, 1978/2007) are integral in social pacification and the creation of docile masses, as they legitimize the continuation of extractivist practices. This subtle aspect of violence, which is especially present in the realm of data extractivism, is crucial as "extractive violence does not always involve armored vehicles, riot police and helicopters" (Dunlap and Jakobsen, 2020, p. 9).

For these reasons, it is important to look at expanded concepts of extractivism to better understand new encroachments that destroy or radically alter lived environments. In this chapter we contemplate the forms of violence that result from the progressively intricate knots that digital technologies weave into different formations of extraction and accumulation. We are sympathetic to the proliferation in the use of the concept of extractivism, as scholars and activists seek to better understand new encroachments by a variety of actors, including: corporations; old and new elites; the multi-billionaires of the digital and financial spheres; progressive governments; actors behind complex investment tools such as churches and pension funds; and even environmental non-governmental organizations engaged in green-grabbing conservation initiatives.

Extractivisms: Digitized and Datafied

The collection, manipulation, and deployment of data are excellent examples of how extractivist processes are useful to describe practices beyond direct natural resource extraction. Data extractivism is a part of a wider self-reinforcing total extractivism that operates at multiple levels within the modern world system, connecting extractivism of natural resources to the extractivism of our thoughts and identity through data (see Figure 9.1).

Before looking at the direct link to natural resources, and the ways extractivism and violence express themselves at different levels of data collection and usage, it is worthwhile briefly to review the terminology. As this is a burgeoning area of study, it is easy to conflate the terms "data" and "digital." As a result, it is important to take a moment to differentiate data collection from other types of digital extractivisms.

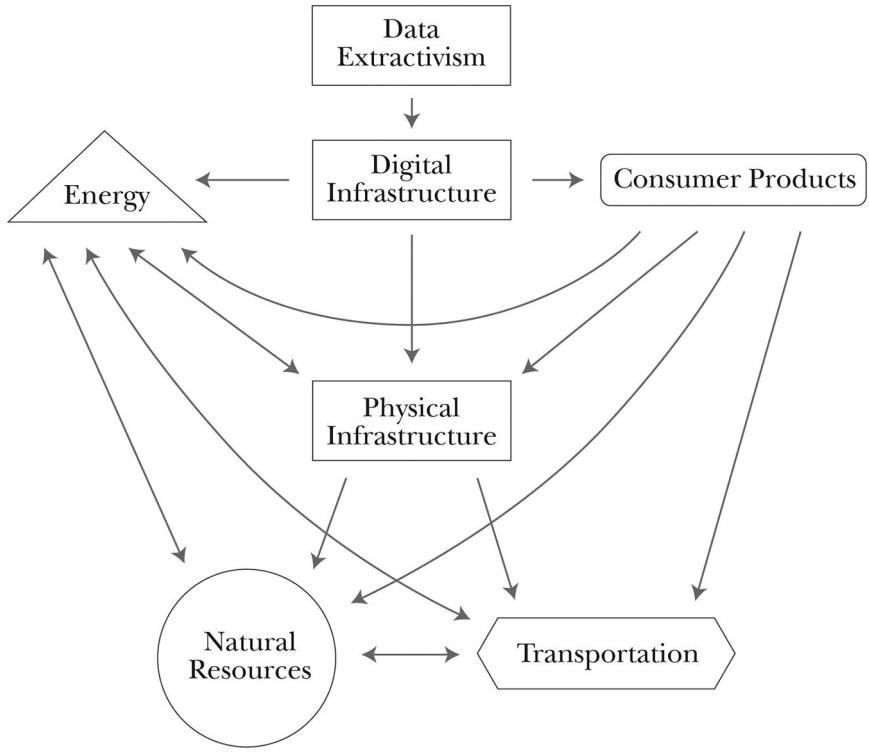

FIGURE 1 This figure illustrates our conceptualization of the web that connects data and natural resource extractivisms. The arrows indicate the lines or directions of dependence; for example Data Extractivism is dependent on Digital Infrastructure.

The definition of 'digital' in the Cambridge English Dictionary is: *using or relating to digital signals and computer technology*, with the business definition adding in: *especially the internet*. This definition can relate to a plethora of tools, spaces, and resources that are quite varied. According to Couldry and Mejias, data is "information flows that pass from human life in all its forms to infrastructure for collection" (2019, p. xiii). So, while data extractivism certainly falls under the umbrella of digital extractivism, they are not synonymous terms. For example, cryptocurrency mining or gold farming are other varieties of digital extractivisms not directly linked to the manufacture and harvesting of personal data (see Table 9.1). Further investigation into types of digital extractivism is beyond the scope of this chapter, as they have very different processes, mechanisms, and outcomes from personal data extraction.

Data extractivism is one of the newest cogs in the self-reinforcing machine of total extractivism (Dunlap and Jakobsen, 2020). It pushes the rationales and destruction of extractivism into our daily lives, as people, their movements, thoughts, and even social connections become the product (Couldry and Mejias, 2019).

TABLE 9.1 Delineating types of digital extractivisms

Type of Extractivism	*Object of Extraction*	*Mode of Extraction*	*Who Profits*
Data Extractivism (Sadowski, 2019)	Personal data	Any sort of internet usage, social media, geotracking, voice pickup, among others. Data points are collected and combined to be packaged and used or sold.	Big tech companies, data brokers, social media, and the companies that produce the infrastructure for data collection.
Gold Farming (Heeks, 2008; Gago and Mezzadra, 2017)	Currency, Items, and Characters in Massively Multiplayer Online Games	Individuals working in a game for extremely long hours to collect resources and level up characters. These resources and characters are then sold directly to people for real money.	A boss, company, or government keeps most of the profits.
Cryptocurrency Mining (Smith, 2019; Rosales, 2019)	Cryptocurrency	Large numbers of energy-intensive computer banks working constantly on extremely complicated algorithms in order to produce cryptocurrency "coins."	Owner(s) of the computer banks. This could be individuals, companies, governments, or other organizations.

Note: There are at least three extractivisms that are digital in nature but utilize extremely different modes of extraction for their respective resources. This is not meant to be exclusive, but rather is a starting point for further exploration.

Data extractivism has a fundamental connection to natural resource extractivism. The growing use of the digital infrastructure for harvesting data, like Google, WeChat, and other social media, drives demand for the physical infrastructure and energy required to utilize those platforms; this, in turn, drives other extractivisms (Dunlap and Jakobsen, 2020). The manufacture of the consumer products relies on the extraction of rare earth elements and other raw materials. In addition, the movement of the parts and finished products across the globe relies largely on fossil-based energy. Beyond the active life of the products needed to interact with the digital infrastructure, there are the issues of the waste, pollution, and human exploitation that attend the disposal of old and broken devices. This is a fundamental, though broad, connection to the violences against the environment, humans, and non-human-beings arising from other forms of resource and energy extraction and extractivism. There is also the material aspect of the ever-expanding physical infrastructure that is needed to keep the digital infrastructure operational (e.g. fiber optic cables, power transmission lines, towers, data farms, and satellites, among the myriad other physical items) and their knock-on impacts on life and the environment (Parks and Starosielski, 2015). As a result, digital infrastructures depend on natural resource extraction, while at the same time natural resource extraction is increasingly driven by the digital—especially data.

Data extractivism involves a type of violence associated with even the most basic collection of data, namely lack of consent. One of the major hallmarks of data extractivism is that there is no meaningful agreement to the harvesting of information. The most common way companies exploit this is the end-user licensing agreement or the Terms of Service of most programs, websites, and devices. These agreements are often designed to be long and difficult to read, and can hide clauses that revoke the rights of users to use or be compensated for their data. The complicated nature of these agreements effectively leaves the user with no power and few alternatives. One must either agree to the terms, and thus give up rights to the data generated by use of the product, or not use the product at all (Sadowski, 2019). This can be seen as a form of accumulation by dispossession, which is based on appropriating resources at zero or very low costs (Harvey, 2003). Couldry and Meijas (2018) even go so far as to suggest parallels between required consent in a website's Terms of Service and the Spanish empire's *Requerimiento*, in which the conquistadors recited an incomprehensible dictum—in the presence of a notary—demanding the acceptance of colonial rule or face violence (see de Vitoria, 2010). Both situations, they argue, require a legally recognized monopoly of force. In the *Requerimiento* it was physical force, whereas with data it is a concentration of economic power, in that, "Whatever the form of force used, its effect now, as then, is through the discursive act that accompanies it to embed subjects inescapably into relations of colonization" (Couldry and Meijas, 2018, p. 341). In this process of legally coerced consent, the conditions for various manifestations of violence are established.

The potential for new forms of extractivist violence is spreading exceptionally fast precisely because these forms are not direct, explicit, or widely recognized. Rather, they are based on a logic of alluring hegemonic expansion wherein the subjects give consent to being targets of extraction, in exchange for using the digital infrastructure, whether it be for work, entertainment, or communication, among the myriad other uses of the digital infrastructure (Van Dijck, 2014). To date, much of the literature on extractivism has overlooked extraction that occurs in the digital realm. This could be due to the notion that extraction is an act that occurs only with and in the material realm, and the digital realm operates apart from the material realm. However, it is convincingly argued that the digital realm and the material realm (or non-digital realm), are in practice, one and the same (see, for example, Horst and Miller, 2012; Pink *et al.*, 2016). In understanding the digital as an extension of the life-world rather than as a separate sphere "out there," the types and possibilities of violence are found to increase in complexity, often becoming obscured or latent, and showing up in ways seemingly far removed from a colloquial conceptualization of the digital.

Moving beyond the ways that infrastructures drive other extractivisms and the ways in which violences are inflicted on the creators of data by simply interacting with the system, data extractivism leads to other socio-environmental damage. There are pollution-like effects on the broader social fabric connected to the way people communicate and how communication is shared in the digital era. Online

environments are constructed to a certain extent solely to extract data; for example, social media has been found to be addictive, and former employees of social media companies have claimed they are designed to be addictive (Andreassen *et al.*, 2012; Andersson, 2018; Schwär and Moynihan, 2020). The fundamental design of these digital interactive spaces makes it easier to create an echo chamber and cut out people who disagree with or are different from the user. This turns dissenting voices into faceless "others." Violence is laced in multifarious ways through these processes and while not immediately apparent, it is always immanent. In order to explore these myriad effects and their accompanying violences, it is worthwhile to look at the resources and processes through which data extraction occurs.

Subtle but Violent

The confounding aspect of data extractivism is that a single piece of data is virtually worthless, but the more that pieces of data are combined, the more valuable the data. The products that follow from the data grow exponentially, allowing a new configuration of information (Sadowski, 2019). One of the most common uses of data—and one of the biggest drivers of its potential violences—is the creation of what are called "data doubles." These abstracted versions of people are created using pieces of data collected from one or a variety of sources through a process that Haggerty and Ericson (2000) describe as a surveillant assemblage. An individual will generally have multiple data doubles, each created by different companies and networks, using data both proprietarily extracted and purchased. Although attached to individuals, the use of the data double is not strictly tailored to the individual—instead it is cross-referenced using Artificial Intelligence (AI) with other data doubles to come up with recommendations and ideas based on probability (Couldry and Mejias, 2019). For example, if you search for a video on YouTube, the suggestions for following videos will be based on what data doubles similar to your own search for or click on next.

The pervasive use of this system—and companies' increasing reliance on the system—can lead to a variety of violences. Some are deeply personal, but hard to predict, because they can impact the growth and development of individuals, and impacts could theoretically be greater on younger generations who might grow up more dependent on this technology. This relates to potential loss of autonomy through a greater dependence not only on technology, but also on AI to handle basic tasks even within technology. For example, finding new music by listening to the radio compared with Spotify with custom playlists, or learning about politics or science by talking with different people and going to lectures compared with an infinite list of suggested videos on YouTube. While it is not always obvious in the face of being fed a seemingly endless stream of content, this dependence could hinder the ability to find new things and escape algorithmically created echo chambers. Data doubles can also relate directly to discrimination and violence, such as with the phenomenon of cybervetting, which occurs when companies examine data doubles from individuals as part of a hiring process, including going into

personal data unrelated to the position. This has led to some expectations of individuals to discuss, unprompted, past issues which could be discernible from their data double. While some companies hail this technology as a boon for streamlining, the ability to allow for stronger gatekeeping and discrimination based on unrelated activities is clear (Hedenus and Backman, 2017). In this way, the data revolution of past decades has ushered in a new era that permeates different spheres of life, extracting knowledge through an extractivist logic imbued with multiple forms of violence.

The interplay between AI and data doubles gives rise to most of the uses of data in data extractivism. Data doubles, once compiled, are used and referenced by AI as the informational basis for completing tasks. However, different AIs work with different types of data, depending on the task. It should be noted that AI is not inherently nefarious; it depends on the intentions of the people and corporations creating the AI. As a tool of extraction in the accumulation, processing, circulation, and usage of data, AI has resulted in variegated forms of violence, giving rise to concepts like 'data violence' (Hoffmann, 2018) and "algorithmic violence" (Onuoha, 2018). These concepts are related to Galtung's concept of structural violence, wherein social structures and institutions perpetuate a form of violence by preventing people from meeting their fundamental needs (2018). Data and algorithmic violence center around how the algorithms that drive automated AI decision-making can perpetuate and deepen violences such as inequalities, segregation, racism, and sexism. This is not *necessarily* intentional—although it can be—but at the very least it occurs because the people designing the AI have underlying structural biases they are unaware of—or do not have a good grasp of the issues they are programming into the AI—and do not understand the best methods and sources for gathering relevant data.

There are already numerous examples of data and algorithmic violences, whether intentional or unintentional. Eubanks (2018) discusses how the automation of decision-making can impact access to life-saving health and social support, which disproportionately hurts impoverished communities. Safransky (2019) argues that data-driven city planning in "smart cities," brought in to make decision-making seem politically unbiased, has in effect recreated the racially discriminatory practice of redlining and unwittingly enforced informal segregation. There is the example of crime prediction software, which tries to foresee the likelihood of crimes occurring in different places in order to inform police patrols. However, they often use datasets that are of poor quality and racially biased. As such, these measures have not been linked to more efficient policing. Rather they have been linked to racial profiling and police harassment of minorities (Mooney and Baek, 2020).

These violences are not limited to the governmental sphere, but also go into the tools of everyday digital life. Facebook AI has a history of discriminating against Native American users by flagging their names as fake, banning them, and requiring the banned individuals to provide multiple forms of identification to customer service before they are reinstated (Holpuch, 2015). In a gross example, Google AI has projected racism by incorrectly automatically tagging pictures of black people as gorillas (Guynn, 2015). Amazon was found to be using AI to identify impulse

buyers and charge them more than non-impulse buyers for the same products, because it was assumed that they were less likely to do research on prices or notice a price hike (Zittrain, 2008). When Amazon's foray into facial recognition AI was turned to photos of members of the U.S. Congress, it misidentified 28 of the congress people as being people from publicly available police mugshots. In this incident, the AI disproportionately misidentified the Black and Latino congress people (Singer, 2018).

Overall, data extractivism has a strong connection with a variety of violences. In the way that it drives other types of extractivism by increasing demand for energy and resources, it drives and exacerbates the violences of those extractivisms. There is violence in the way that companies force data creators to "consent" to their data being extracted, or else be unable to use these vital systems. There is damage and violence in the way that data doubles are used to limit our interactions, opportunities, and choice. There is data/algorithmic violence built into AI that informs our governments and drives our engagement in digital spaces. These violences and depletions are insidious; they grow in impact as technology embeds itself deeper into our lives, and generations begin to grow up with no conception of what life could be like without these intrusions.

Digital Violence IRL

For proponents of limiting the lens of extractivism strictly to natural resources, one of the major criticisms of including the resource of data is that the associated/caused violences are only online and do not spill over IRL (to use the internet parlance, "In Real Life" or the everyday physical world). Although the previous section touched on ways that data/algorithmic violence can easily leap over into physical violence, it is worthwhile to touch on some more concrete examples of the intrusion, manipulation, and literal violence that have grown from the products and methods of data extractivism, as well as the toxic social environment that it creates.

The Chinese context provides some interesting examples, as Chinese companies have been at the forefront of developing and rolling out facial recognition infrastructure and AI (Simonite, 2019). This context provides some of the most famous and extensive examples of how facial recognition technology can spread into many facets of public life. Issues of consent, collection, and usage of data have mixed the digital with the physical world via the usage of facial recognition technology. The people who are having their faces recognized and processed while they walk down the street have little idea of where the data is going, and give no direct consent. There are even government mandated regulations that require facial recognition scans to be able to engage with certain technologies and products, for example signing up for a sim card or internet service (Kuo, 2019). In many workplaces, employees are required to clock in using facial recognition with little or no knowledge of where that data goes (Borak, 2019). Facial recognition can even be used to order and pay for fast food (Hawkins, 2017).

Stepping out from consent, the consequences of facial recognition come into the real world. In some Chinese cities, facial recognition technology has been installed to prevent jaywalking—by effectively doxing, or collecting transgressors' personal information with malicious intent. This is done by using facial recognition technology to project the faces of jaywalkers on billboards as well as showing their pictures, names, and partial identification (ID) numbers on a traffic police website. There is also discussion of expanding the system to automatically text fines to the mobile phones of jaywalkers via social media platforms (Li, 2018). While the thought of official doxing might be unnerving, the case gets far more intrusive and dystopian when looking at the usage of surveillance cameras in Xinjiang (where the Uighur minority group makes up a majority of the population), where facial and ID recognition, as well as mandatory checkpoints, follow people wherever they go. An unsecured database of a surveillance company in the city Urumqi, Xinjiang was found to have facial recognition records and ID scans for 2.5 million of the 3.5 million inhabitants of the city (Buckley and Mozur, 2019). Given the rollout of this level of surveillance via facial recognition and the start of reeducation camps, detaining up to 1 million Uighurs, it is hard to ignore how data can create violence outside the confines of the purely digital realm (Mozur, 2019).

This is not to say that this spillover is a uniquely Chinese issue; it is a global one. Beyond the examples of the previous section, the pervasiveness of the QAnon conspiracy theory and actions inspired by it show how the addictive infrastructure for data extraction and the socially toxic environment it creates can have ramifications outside of the digital realm. This includes in 2016 when a man was inspired by the conspiracy and online echo chambers to drive hundreds of kilometers with an assault rifle, handgun, and knife to a Washington, DC pizza restaurant. His aim was to free victims of left-wing elite child trafficking that the conspiracy said were being held and ordered there; he held people hostage at gunpoint for hours and discovered that there were no secret passages before being arrested (Robb, 2017). We also see U.S. politicians making references to the conspiracy and the spread of the conspiracy to other parts of the world (Stanley-Becker, 2020; Bradley *et al.*, 2020).

Although these are some quick snapshots, there are innumerable examples of how data extractivism and the toxic environment that it creates can cause violence to spill over into the physical realm in a visceral way. These examples are only likely to increase as tools of data extractivism push further into our lives, and the digital and non-digital realms become increasingly—perhaps inextricably—enmeshed.

Conclusion

This chapter has outlined how the lines between realms of extraction have become blurred. As a result, and as the literature cited in this article shows, there is a clear effort by a rising number of scholars to understand the entanglements of datafied and digitized formations of extractivism as they bind with more established notions, processes, and practices of extractivism. There is a need for a deeper and critical

analysis of the rich complexities of the interface of natural resource, digital, and intellectual extractivisms to unveil the complex web of extractivisms in this era. This chapter has provided some initial thoughts on the violences manifest in and through these newer configurations of extractivism(s). There is still much ground to cover in utilizing extractivism(s) as a tool to provide systemic understandings of our extractive age, and much additional research needs to be done, but as the other chapters in the volume demonstrate, the conceptual work is already well underway.

References

Andersson, H. (2018) 'Social Media Apps Are "Deliberately" Addictive To User', BBC News. Available at: www.bbc.com/news/technology-44640959.

Andreassen, C., Torsheim, T., Brunborg, G., and Pallesen, S. (2012) 'Development of a Facebook Addiction Scale', *Psychological Reports*, 110 (2), pp. 501–517.

Borak, M. (2019) 'Man Mistaken For His Co-Workers Illustrates The Flaws Of Facial Recognition', *South China Morning Post*. Available at: www.scmp.com/abacus/tech/article/3029424/man-mistaken-his-co-workers-illustrates-flaws-facial-recognition.

Bradley, M., Angerer, C., and Suliman, A. (2020) 'Qanon Supporters Join Thousands At Protest Against German Coronavirus Rules', NBC News. Available at: www.nbcnews.com/news/world/qanon-supporters-join-thousands-protest-against-germany-s-coronavirus-rules-n1238783.

Buckley, C. and Mozur, P. (2019) 'How China Uses High-Tech Surveillance To Subdue Minorities', *The New York Times*. Available at: www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.htm.

Couldry, N. and Mejias, U. (2018) 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject', *Television & New Media*, 20 (4), pp. 336–349.

Couldry, N. and Mejias, U. (2019) *The Costs Of Connection: How Data Is Colonizing Human Life And Appropriating It For Capitalism*. Stanford, CA: Stanford University Press.

de Vitoria, F. (2010) *Political writings* (A. Pagden and J. Lawrance, eds). Cambridge: Cambridge University Press.

Dowbor, L. (2018) *The Age of Unproductive Capital: New Architectures of Power*. Cambridge: Cambridge Scholars Publishing.

Dunlap, A., and Jakobsen, J. (2020) *The Violent Technologies of Extraction: Political Ecology, Critical Agrarian Studies and the Capitalist Worldeater*. London: Palgrave MacMillan.

Eubanks, V. (2018) *Automating Inequality*. New York, NY: St. Martin's Press.

Foucault, M. (1978/2007) *Security, Territory, Population: Lectures at the Collège de France 1977–78*. London: Palgrave Macmillan.

Gago, V. and Mezzadra, S. (2017) 'A critique of the extractive operations of capital: Toward an expanded concept of extractivism', *Rethinking Marxism*, 29 (4), pp. 574–591.

Gudynas, E. (2018) *'Extractivisms: Tendencies and Consequences' in Munck, R. and Wise, R.D. (eds.) Reframing Latin American Development*. New York, NY: Routledge.

Guynn, J. (2015) 'Google Photos Labeled Black People "Gorillas"', Eu.usatoday.com. Available at: https://eu.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465.

Haggerty, K. and Ericson, R. (2000) 'The surveillant assemblage', *British Journal of Sociology*, 51 (4), pp. 605–622.

Harvey, D. (2003) *The New Imperialism*. Oxford: Oxford University Press.

Hawkins, A. (2017) 'KFC China Is Using Facial Recognition Tech To Serve Customers – But Are They Buying It?', *The Guardian*. Available at: www.theguardian.com/technology/2017/jan/11/china-beijing-first-smart-restaurant-kfc-facial-recognition.

Hedenus, A. and Backman, C., (2017) 'Explaining the Data Double: Confessions and Self-Examinations in Job Recruitments', *Surveillance & Society*, 15 (5), pp. 640–654.

Heeks, R. (2008) 'Current Analysis and Future Research Agenda on "Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games', *Development Informatics Working Paper*, (32), Available at: http://dx.doi.org/10.2139/ssrn.3477387.

Hoffmann, A. (2018) 'Data Violence And How Bad Engineering Choices Can Damage Society', *Medium*. Available at: https://medium.com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4.

Holpuch, A. (2015) 'Facebook Still Suspending Native Americans Over "Real Name" Policy', *The Guardian*. Available at: www.theguardian.com/technology/2015/feb/16/facebook-real-name-policy-suspends-native-americans.

Horst, H. A. and Miller, D. (2012) *Digital Anthropology*. London: Berg.

Kröger, M. (2013) *Contentious Agency and Natural Resource Politics*. London: Routledge.

Kröger, M. (2020) *Iron Will: Global Extractivism and Mining Resistance in Brazil and India*. Ann Arbor, MI: University of Michigan Press.

Kuo, L. (2019) 'China Brings In Mandatory Facial Recognition For Mobile Phone Users', *The Guardian*. Available at: www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users.

Li, T. (2018) 'Just Jaywalked? Check Your Mobile Phone For A Message From Police', *South China Morning Post*. Available at: www.scmp.com/tech/china-tech/article/2138960/jaywalkers-under-surveillance-shenzhen-soon-be-punished-text.

Malm, A. (2016) *Fossil Capital: The Rise of Steam Power and the Roots of Global Warming*. London: Verso Books.

Mezzadra, S. and Neilson B. (2017) 'On the multiple frontiers of extraction: Excavating contemporary capitalism', *Cultural Studies*, 31 (2–3), pp. 185–204.

Mooney, T. and Baek, G. (2020) '*Is Artificial Intelligence Making Racial Profiling Worse?*', Cbsnews.com. Available at: www.cbsnews.com/news/artificial-intelligence-racial-profiling-2-0-cbsn-originals-documentary.

Moore, J.W. (2018) 'The Capitalocene Part II: Accumulation by appropriation and the centrality of unpaid work/energy', *The Journal of Peasant Studies*, 45 (2), pp. 237–279.

Mozur, P. (2019) 'One Month, 500,000 Face Scans: How China Is Using A.I. To Profile A Minority', *The New York Times*. Available at: www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

Onuoha, M. (2018) 'Notes On Algorithmic Violence', GitHub. Available at: https://github.com/MimiOnuoha/On-Algorithmic-Violence.

Parks, L. and Starosielski, N. (2015) *Signal Traffic: Critical Studies of Media Infrastructures*. Champaign, IL: University of Illinois Press.

Pink, S., Ardevol, E., and Lanzeni, D. (eds.) (2016) *Digital Materialities: Design and Anthropology*. London: Bloomsbury Academic.

Robb, A., (2017) '*Pizzagate: Anatomy Of A Fake News Scandal*', *Rolling Stone*. Available at: www.rollingstone.com/feature/anatomy-of-a-fake-news-scandal-125877.

Rosales, A. (2019) 'Radical rentierism: Gold mining, cryptocurrency and commodity collateralization in Venezuela', *Review of International Political Economy*, 26 (6), pp. 1311–1332.

Sadowski, J. (2019) 'When data is capital: Datafication, accumulation, and extraction', *Big Data & Society*, 6 (1), pp. 1–12.

Safransky, S. (2019) 'Geographies of Algorithmic Violence: Redlining the Smart City', *International Journal of Urban and Regional Research*, 44 (2), pp. 200–218.

Schwär, H. and Moynihan, R. (2020) 'Instagram And Facebook Are Intentionally Conditioning You To Treat Your Phone Like A Drug', *Business Insider*. Available at: www.businessinsider.com/facebook-has-been-deliberately-designed-to-mimic-addictive-painkillers-2018-12?r=US&IR=T.

Segura, M.S. and Waisbord, S. (2019) 'Between data capitalism and data citizenship', *Television & New Media*, 20 (4), pp. 412–419.

Simonite, T. (2019) 'Behind The Rise Of China's Facial-Recognition Giants', Wired. Available at: www.wired.com/story/behind-rise-chinas-facial-recognition-giants.

Singer, N. (2018) 'Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says', *The New York Times*. Available at: www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.

Smith, H. (2019) '*The Shady Cryptocurrency Boom On The Post-Soviet Frontier*', Wired Available at: www.wired.com/story/cryptocurrency-boom-post-soviet-frontier.

Stanley-Becker, I. (2020) 'How The Trump Campaign Came To Court Qanon, The Online Conspiracy Movement Identified By The FBI As A Violent Threat', *The Washington Post*. Available at: www.washingtonpost.com/politics/how-the-trump-campaign-came-to-court-qanon-the-online-conspiracy-movement-identified-by-the-fbi-as-a-violent-threat/2020/08/01/dd0ea9b4-d1d4-11ea-9038-af089b63ac21_story.html.

Thatcher, J., O'Sullivan, D., and Mahmoudi, D. (2016) 'Data colonialism through accumulation by dispossession: New metaphors for daily data', *Environment and Planning D: Society and Space*, 34 (6), pp. 990–1006.

Van Dijck, J. (2014) 'Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology', *Surveillance & Society*, 12 (2), pp. 197–208.

Zittrain, J. (2008) *The Future of The Internet – And How to Stop It*. London: Penguin UK.